

A B S T R A C T

5 The invention relates to a method of automatically
classifying alerts issued by intrusion detection sensors
(11a, 11b, 11c) of an information security system (1) for
producing collated alerts, each alert being defined by a
plurality of qualitative attributes (a_1, \dots, a_n) belonging to
a plurality of attribute domains (A_1, \dots, A_n) , which method
10 comprises the following steps:

- organizing the attributes belonging to each
attribute domain into a hierarchical structure;
- constructing for each alert issued by the
intrusion detection sensors (11a, 11b, 11c) a trellis
15 specific to that alert by generalizing each alert in
accordance with each of its attributes and at all the
levels of the hierarchical structure;
- iteratively merging each specific trellis into a
general trellis;
- 20 · identifying collated alerts in the general trellis
by selecting the alerts that are simultaneously the most
pertinent and the most general; and
- supplying the collated alerts to an output unit
(23) of an alert management system (13).

25

30

Translation of the title and the abstract as they were when originally filed by the
Applicant. No account has been taken of any changes that may have been made
subsequently by the PCT Authorities acting ex officio, e.g. under PCT Rules 37.2,
38.2, and/or 48.3.